



DEPARTMENT OF THE ARMY
UNITED STATES ARMY GARRISON HEIDELBERG
UNIT 29237
APO AE 09102-9237

IMEU-HEI-ZA

21 April 2006

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: United States Army Garrison Heidelberg (USAG Heidelberg) Command Policy Memorandum # 50, Installation Access Control

1. Reference: Army in Europe Regulation 190-16, 22 Mar 05. Other references are shown in the enclosed procedure.
2. This policy provides guidance for access controls within the USAG Heidelberg and its outlined Garrisons. It applies to anyone with legitimate need to access USAG Heidelberg installations, except to restricted areas governed by other regulations. The policy accomplishes the following:
 - a. Contains guidance for areas not specifically covered in Army in Europe (AE) Regulation 190-16. These procedures and responsibilities are described in the enclosed procedure.
 - b. Ensures compliance with Force Protection Condition (FPCON) measures related to access control. It prohibits the unlawful introduction of weapons, explosives, or other contraband onto USAG Heidelberg installations.
 - c. Facilitates the identification of barred individuals and individuals not entitled access to USAG Heidelberg installations, and assists in the prevention of wrongful appropriation and pilferage of government property.
 - d. Incorporates the Installation Access Control System (IACS).
3. Access to USAG Heidelberg installations will be strictly enforced. To ensure installation security, the policy and procedures of this memorandum may change because of conditions in the baseline force protection posture. The policy and procedures will not be supplemented. Local SOPs are authorized to specify local procedures, which cannot be less restrictive than this policy or AE Regulation 190-16.

Encl
Installation Access Control Procedures

/s/
WILLIE E. GADDIS
Colonel, AV
Commanding

Installation Access Control Procedures

1. Responsibilities

a. USAG Heidelberg Provost Marshal:

- (1) Serve as the proponent for all policy matters pertaining to access control.
- (2) Conduct staff assistance visits and command inspections to ensure that the installation access control policy, IACS Department of Defense (DOD) identification card (ID) card registration and installation pass issuing procedures are followed correctly.
- (3) Consolidate and forward all USAG Heidelberg and Tailored Garrison bar lists to USAREUR Office of the Provost Marshal (OPM).

b. Tailored Garrison Commanders are responsible for the security of their installations. Inconvenience to an individual is not a reason to circumvent or modify the procedures established by this policy. They will:

- (1) Comply with the responsibilities outlined in Army in Europe (AE) Regulation 190-16, § 5g.
- (2) Ensure each Installation Access Control Officer (IACO) establishes Standard Operating Procedures (SOPs) that outline the daily operations including the specific and implied duties of their office personnel.
- (3) Issue special guard order procedures to comply with AE Regulation 190-16 and this Supplemental policy.
- (4) Approve all applications for Tailored Garrison-wide installation passes having derogatory information in accordance with (IAW) AE 190-16, § 30b (5). This authority has been delegated by the USAG Heidelberg Commander. Ensure that IACOs are only accepting properly approved derogatory information.
- (5) Outline procedures for access of various types of vehicles and personnel at the various Force Protection Conditions (FPCON) IAW higher headquarters directives.
- (6) Outline procedures for allowing access to large groups.
- (7) Ensure clearing papers for civilian and military include processing in person with respective IACO, vehicle registration and PMOs.

(8) Establish and publicize time limits for the duration of guest visits.

(9) Outline procedures to allow for the reconciliation of sign-in rosters every 24 hours. These will include procedures for contacting sponsors who appear to have violated the policy and for verification of the current status of the guest.

(10) Establish a minimum of one IACO primarily responsible for issuing installation passes. Additionally, there will be a registration station within the Tailored Garrisons central in processing facility (CPF), or at least on the same installation, responsible to register and de-register DOD ID card holders.

c. Sponsoring Organizations:

(1) Comply with all responsibilities outlined in AE Regulation 190-16, § 5 k.

(2) Prepare AE Form 190-16A IAW AE Regulation 190-16, § 30, for all existing installation pass holders and new installation pass applicants, for them to register into the IACS system. Sponsors must ensure each pass applicant receives only the level of access absolutely required. Access to installations must be based on definitive operational need and not on supposition or tentative information.

(3) Prepare memorandum for local Tailored Garrison Provost Marshal requesting Military Police background checks on all personnel who require those, IAW person categories outlined in AE Regulation 190-16, § 13-29. (Example 2a)

(4) Provide IACOs with new sponsoring official's memorandum. See appendix B, AE Regulation 190-16.

(5) Will ensure that if sign-in authority is requested, that it is authenticated by the commander of the unit or director of the division/organization.

(6) Individuals requiring Local National Screening (LNS) will not be issued any access document until the sponsor verifies on the application if the background check has been initiated or completed (AE Form 604-1A, Personnel Data Request). The sponsor must also enter in the pass application the date of initiation or completion of the background check (AE Form 190-16A, Application for USAREUR/USAFE Installation Pass).

(7) Sponsoring officials will ensure vehicle registration information is included on the application for all vehicles an applicant routinely drives onto the installation.

(8) Sponsoring organization will ensure that appropriate level of adjudication is received for the type of pass requested.

2. General Procedures.

a. Pass Issuing: Tailored Garrison level IACOs will issue all levels of passes to include USAREUR level passes. All IACOs can register or de-register any DOD ID cardholder or installation pass holder; however, Central Processing Facilities (CPFs) will be responsible for issuing installation passes to family members only, and will register and de-register only those personnel who possess a DOD ID card. Temporary installation passes are not authorized for USAREUR-wide access.

b. Quarterly Reconciliation: Each IACO will conduct a quarterly reconciliation with each sponsoring organization to ensure the IACS database accurately reflects individuals identified as current by the sponsoring organization. IACOs will maintain a copy of these reconciliations on file for one year.

c. School Bus Drivers: All school bus drivers must have a valid installation pass to be allowed entrance to any USAG Heidelberg installation. School bus drivers with a valid installation pass can vouch for all students on the bus (FPCON A and B only). Any non-student, (such as bus monitors), on the bus must present their ID card. Those drivers that do not have a valid installation pass must be escorted while on the installation.

d. Tour Buses: Tour buses present an access challenge. In order to be allowed unaccompanied access, the tour bus driver must produce a manifest which includes time, date, and location of personnel pickup for an authorized tour upon initial entry to an installation (first pick-up). When a bus arrives from another installation, all occupants will be authorized access upon presenting a valid access document. Guards at Access Control Points (ACP) will check 100% of all passengers for valid access documents. Personnel without valid access document(s) must be signed onto the installation.

e. Other: There are two categories for buses that transport military personnel:

(1) Buses driven by military personnel: The Senior Military person in the bus may vouch for all soldiers in the bus and will provide his/her ID to the guard.

(2) Buses driven by a contractor: The Senior Military person in the bus may vouch for all soldiers in the bus and will provide his/her ID to the guard. The contractor must provide a valid Installation Pass or ausweiss (if needed to be signed-in).

f. Delivery Personnel: Delivery personnel (pizza, Chinese food, etc.) must have an installation access document issued and in their possession in order to gain access to the installation (§ 17, AE Regulation 190-16). These personnel will not be signed onto the installation except when applying for an installation pass. This does not pertain to parcel or correspondence deliveries, i.e., FedEx, UPS, Bundespost or scheduled vendor deliveries, i.e.,

AAFES, commissary. Those delivery personnel not meeting the definition of § 17(a), AE Reg 190-16 can be signed onto the installation, example: AAFES Vendor, FedEx, UPS.

g. Access by Children:

(1) Children under 10 years of age are allowed access to all USAG Heidelberg installations when accompanied by a person with an authorized DOD ID card, or is listed on an approved access roster.

(2) If a child is in possession of a Kinderausweiss and has a need for recurring access due to volunteer work, membership of an organization, etc., the Tailored Garrison Commander may consider issuing an installation pass.

h. Local National (LN) Parents of DOD ID Card Bearing Children:

(1) Parents who are local national residents of DOD ID card bearing children require special consideration. If the parent intends to exercise the child's privilege of shopping on the installation, they are required to obtain customs approval through the USAREUR 7/A Office of the Provost Marshal, Host Nation Customs Policy Branch, telephone number: DSN 381-8141 /7354 (commercial 0621-730-8141). They must attach a copy of the customs approval with their application.

(2) Access will be for those installations, plus medical facilities, that house the facilities that they are authorized to enter. If they are not exercising the shopping privilege, then their access will be only for the installation where the child receives his/her primary health care.

(3) The person category will be "other".

(4) Time and date will be "Monday through Friday" for normal business hours (0800-1700)

(5) No sign-in privileges will be authorized.

(6) Required background checks, at a minimum, will be Police Good Conduct Certificate (PGCC) and local Military Police (MP) Check.

i. Sponsoring Official's Memorandum: Each sponsoring official must sign the memorandum under his/her name to provide a signature for comparison with the application memorandums. Once the application memorandum is completed, the sponsoring official will escort the applicant to the servicing IACO to obtain their installation pass. The applicant must bring all required documentation, e.g., proof of LNS submission, MP record check, PGCC.

j. Military Formations: Personnel conducting physical fitness outside of an installation do not required to provide an ID as long as they are in a formation. The Senior NCO or Officer in charge of the formation can vouch for all personnel in the formation.

3. Access Control Point Procedures.

a. Search Authorization: Any vehicle or person attempting to access a USAG Heidelberg installation is subject to search IAW AR 190-22 and USAREUR Supplement 1 to AR 190-22.

b. Access Verification: Guards will stop all vehicles entering USAG Heidelberg installations to verify access documents. Guards will conduct 100% hands on ID checks of individuals desiring access to an installation. All persons who have proper identification will be allowed unescorted access. All individuals who do not have a proper DOD ID card, installation pass, or are not on an access roster must be signed in. See AE Regulation 190-16, § 41. All persons entering USAREUR installations will conform to FPCON or RAM program measures in effect. Guards will utilize access control procedures IAW AE Regulation 190-16, § 44 and local SOPS.

c. Access Authorization: At gates where IACS handheld scanners devices are active, gate guards will scan the bar code of all DOD ID cards and installation passes to ensure that they are valid and that the person is authorized entry. At gates where IACS handheld scanners are not active, identification checks will continue as prescribed in the Special Guard Orders.

(1) Bar List: All individuals requesting to be signed-in will be checked against the USAREUR and USAG Heidelberg bar list. IACS equipped gates will do this automatically. Individuals whose names are on the bar list will be denied access. Anyone on the bar list attempting to gain access with an installation pass or temporary installation pass will be titled with attempted trespassing and the pass will be confiscated. Once IACS is fully implemented all DOD ID cards and installation passes are automatically checked against the bar lists. All attempted entries will be documented in the access control point journal.

(2) Barred Person Entry: Personnel who are barred from installations within the USAG Heidelberg will coordinate entry with the Military Police as instructed in the bar letter (example: retired member with USAREUR-wide bar seeking medical services can be allowed onto the installation where services are available if previously coordinated with Military Police). Possession of a DOD ID card does not override the bar list.

d. Solicitation Permits: Solicitation permits do not authorize facility or installation access to the holder. These permits are issued and controlled IAW AR 210-7 and USAREUR Regulation (UR) 210-7, which gives solicitors authorization to sell merchandise only. Individuals wishing to access a facility or installation must obtain access and solicitation authority from each installation or community as a separate action through each Tailored Garrison Commander IAW AE 190-16, § 18.

e. Emergency Vehicles: Emergency vehicles (US and host nation) are those vehicles with emergency lights plainly visible and clearly marked as being such, i.e. Fire, Police, EOD and Ambulance. When entering USAG Heidelberg installations, the operators of US Forces emergency vehicles will produce a DOD ID card and are required to show a dispatch, drivers' license, or other documents. Host nation Police, in marked vehicles and in uniform, are required to show their Dienstaussweis (service identification card). Other host nation emergency personnel requiring access in a non-emergency mode will show their installation pass, Ausweis (Local National identification card) or service identification document.

f. Emergency Vehicles using Code (in response to an emergency): Emergency vehicles running code (emergency lights and sirens operational) will not be unnecessarily delayed at the ACPs. ACP personnel will stop the vehicle long enough to perform a very quick cursory look to ensure security and safety. ACP personnel will then immediately notify the Military Police Desk after allowing access to any emergency vehicles (US Forces or Host Nation) running code. At a minimum they will report to the MP Desk Sergeant, the number and type of vehicles, the direction of travel and address/area of the emergency.

g. Diplomatic Vehicles: Vehicles with US diplomatic plates will be allowed access after the driver produces a valid installation access document (ID Card, Ausweis, Passport etc). Passengers will not be required to produce identification. The vehicle will not be searched.

h. Installation Access without Authority/Verification: Individuals seeking access to an installation without access authority or documents for reasons, such as seeking employment, access to Staff Judge Advocate (SJA) and Inspector General (IG), or submitting bids at Regional Contracting Office (RCO), etc., must make arrangements prior to arriving at the installation access point. Personnel in this category must be signed in and escorted to and from their destination.

i. Access to Installations Not Authorized: IAW AE Regulation 190-16, § 8a, personnel may obtain access to a installation which they do not have access privileges for by producing either TDY orders or a memorandum signed by their chief, deputy of their organization or directorate.

j. Access for Lost/Stolen Access Documents: Individuals will be allowed unaccompanied access using the verification features of the biometric scan or SSN/ID number search (manual look-up) and comparing the file photo with the individual. Access will be authorized once the individual has been identified. The individual will be instructed to report to the MP station and report the incident.

k. Sign-in Authority for Non-registered DOD ID Card Holder: When a DOD ID Card holder attempts to sign in an individual(s) and is not registered in IACS; they will be informed that they are not allowed sign-in privileges until they have registered.

4. Procedures for Background Checks: All personnel requesting installation passes require certain background checks prior to being issued a pass. AE Regulation 190-16, § 13-29 outlines which background checks are required for the various person categories. The procedures below will be followed in order to obtain the various background checks.

a. Local National Screening (LNS), UR 604-1.

(1) See AE Regulation 190-16, § 13-29, for required person categories.

(2) All Local National (LN) applicants shall present to the sponsoring agency a current Police Good Conduct Certificate (PGCC) from their city of residence that is less than one year old. Applicants will also be required to provide a completed UR 604-1B form, legible and signed, containing their birth information and residence history dating back a minimum of 10 years.

(3) The sponsoring organization is responsible for initiating all Local National Screening on its prospective employees. The sponsor will go to the following web site: www.dcsintweb.hqusareur.army.mil/LNSP2/ and initially register into the program and be issued a login and password to access the on-line background screening process. The sponsor will then fill out AE Form 604-1A (Personnel Data Request) using the information the applicant provides in the USAREUR Form 604-1B (Personnel Data Worksheet).

(4) LNS required for employment: LN employee and security guard person categories require an LNS be completed for employment. If derogatory information is returned, it is reviewed and employment suitability is determined. Upon completion, these person categories do not require further derogatory review for installation access.

b. Derogatory Information: **Derogatory information will not be transmitted over the NIPRNET.**

(1) Derogatory information will be reported from USAREUR G-2 to the USAG Heidelberg Security Office and its Tailored Garrisons.

(2) The Tailored Garrison Security Office will forward the information to the sponsoring agency. If the sponsoring agency wishes to pursue an installation pass they must complete the Approval/Disapproval Request (Example 3 this procedure) and forward to the proponent office (Example 4 procedure).

(3) Upon review, the proponent office will forward to the approval authority.

(4) After final decision is made, the approval authority will return the request to the sponsoring agency for action.

(5) If installation access is approved, the request must be attached to the application.

c. Police Good Conduct Certificate (PGCC), or Polizeiliches Fuehrungszeugnis, is required prior to issuing the temporary installation pass.

(1) See AE Regulation 190-16, § 13-29, for required person category.

(2) The responsibility to obtain and pay for the PGCC from the Einwohnermeldeamt (Residents' registration office) is the installation pass applicant's. To process the application for a pass without further administrative action, the PGCC must state "Keine Eintragung" at the bottom, which means there is no record of misconduct.

(3) For individuals who have derogatory information on their PGCCs, follow the same procedures as with LNS above.

(4) Persons not permanently residing in Germany must provide the original and a translated copy, into either English or German, of their resident country's national equivalent to the PGCC.

d. Defense Clearance and Investigations Index (DCII): for applicants who have prior US forces affiliation.

(1) See AE Regulation 190-16, § 13-29, for required person category.

(2) The sponsoring official will fill out DA Form 1144 and send it to Commander, USAREUR, ATTN: AEAGB-CI-S, Unit 29351, APO AE 09014.

e. Resident and work permits may be required if the applicant is not a host nation or European Union resident.

(1) See AE Regulation 190-16, § 12-26, for required person category.

(2) The responsibility to obtain resident and work permits, if required, is the pass applicant's. The resident permit is stamped in the passport. The work permit is issued on a separate form.

f. A Military Police check is required prior to issuing the temporary installation pass.

(1) See AE Regulation 190-16, § 12-26, for required person categories.

(2) The sponsoring organization will submit a memorandum to the local Military Police Station requesting a MP check on required applicants. See Appendix B for sample memorandum.

(3) The Military Police will complete all MP checks and make them available for pick-up by the sponsoring organization within five working days. For individuals who have derogatory information on their MP checks, follow the same procedures as with LNS above.

5. Procedures for notifying USAREUR of USAG Heidelberg/Tailored Garrison implemented bars.

a. Tailored Garrison Commanders are responsible for submitting all completed USAG bar actions to USAREUR Office of the Provost Marshal, Security Operations Branch, to update the bar list in IACS.

6. Special event assessment: when an installation is hosting an event where the use of an access roster is not feasible; the tailored garrison commander will submit an activity OPOD that must address anti-terrorism and force protection (AT/FP) security measures and procedures to control visitors on post. This OPOD must be staffed through USAG Heidelberg Director, Plans, Training, Mobilization, and Security (DPTMS) for approval.

7. Procedures for Lost ID cards and passes:

a. When an ID Card or installation pass is lost or stolen the responsible individual will immediately notify their IACO, sponsoring agency, and the MP Desk Sergeant (D/SGT) at the local Provost Marshal office.

b. The MP D/SGT will initiate an immediate flag in IACS so the ID card or pass cannot be utilized to access any installation.

c. The individual will fill out a report of the lost item, which the D/SGT will retain for their official record. The D/SGT will provide the individual a copy of the form.

d. This form must be given to the IACO or ID card section in order to obtain a new ID card or installation pass.

e. The responsible IACO will initiate a lost or stolen notification and de-register the lost or stolen ID card or installation passes in IACS.

f. DOD ID cardholders must go to their ID card office to receive a new ID card and return to the nearest IACO to be registered. A new application from the sponsoring organization will be required for a replacement installation pass. All procedures outlined in AE Regulation 190-16, § 30 and this policy will apply.

g. Installation pass holders must present a PGCC not more than 12 months old to extend the expiration date of their original pass. This is in addition to AE Reg 190-16, § 30, which apply to

application procedures for lost or stolen passes. This does not apply to the local national employee category.

8. Procedures for confiscating ID Cards and Installation Passes:

a. Tailored Garrison commanders will ensure special guard orders thoroughly govern the procedures of this paragraph.

b. Unreadable Bar Codes:

(1) Gate guards can verify if a person is registered into IACS by conducting a manual look-up at the ACP workstation. Those who are positively identified as being registered in IACS will be granted access and instructed to register their current DOD ID card or obtain a new DOD ID card or installation pass immediately. Guards will log this information into their journals to be turned into the local IACO.

(2) When the records search reveals that the individual is not registered in the IACS, guards will confiscate the installation pass IAW AE Regulation 190-16, § 41 and immediately turn it over to the MPs. DOD ID cardholders will be logged in and told to go to the nearest IACO to be properly entered into IACS. Confiscation of the DOD ID card is required only if the card appears to be forged or altered. In this case, guards will contact the MPs. Issue AE Form 190-16b, Receipt for Confiscated ID/Pass.

c. Forgotten ID Cards:

(1) ACP Personnel will confirm authorized access by performing a manual look-up. If an ID Card is confirmed, access will be granted (See procedures in § 3j).

(2) ACP personnel will not grant access to those whom have an expired DOD ID card or installation pass. It is the individual's responsibility to ensure his DOD ID card or installation pass is current and entered into IACS.

d. Confiscation:

(1) All DOD ID cards and installation passes that are expired will be confiscated by ACP personnel or Military Police. ID cards or installation passes that are mutilated, or have illegible identification data or an unrecognizable photo will also be confiscated if the guards cannot positively verify that the individual has authorized access or a second form of picture ID.

(2) Military Police/ACP personnel will receipt for all confiscated ID cards or AE 190-16b installation passes. A copy of this form will be given to the person who presented the card or pass. This receipt IS NOT an access document.

(3) Confiscated installation passes and ID cards will be turned in to the ID card section or Installation Pass Office within 24 hours.

(4) Individuals who have their pass or ID card confiscated must be signed in as a visitor in IACS until a new pass or ID card is issued.

(5) When an individual fails to comply with any directives or orders, or objects to surrendering an ID card or installation pass that has expired, the military police will be notified.

9. Procedures for Registering Privately Owned Vehicles:

a. All Installation Pass holders will register their privately owned vehicles (the vehicles they plan on using to access USAREUR installations) into IACS. There is no limit on the number of vehicles registered.

b. The IACS registrar will enter the vehicle information into the IACS.

c. Contractors will register company vehicles if they are routinely used to access installations. This includes DODDS, DeCA and AAFES contractor vehicles.

10. Security, Inventory and Accountability Requirements and Procedures:

a. IACOs will ensure they comply with all security, inventory and accountability requirements IAW AE Regulation 190-16, § 36c.

b. When not in use or under continuous observation by authorized persons all IACS equipment and supplies will be secured inside a locked room.

c. Keys and locks will be maintained IAW AR 190-51 Appendix D.

d. IACOs will be inspected by the USAG Heidelberg PMO as part of the command inspection program and subject to review by the command Inspector General and Internal Review Office.

11. Sign-in Procedures:

a. Installation pass holders granted sign-in privileges are limited to four persons with their vehicles and are “for official business only.” Persons granted sign-in authority should either be in a supervisory position or have “official need” to ensure mission accomplishment (i.e. COR, project manager, etc.).

b. The sponsor is responsible for the conduct of the individuals they sign-in. Both DOD ID card holders and installation pass holders authorized sign-in privileges must understand this and will maintain control of the personnel at all times.

c. Authorized sponsors signing people in to an installation or housing area must ensure that their guests are signed out. When possible, guests should be signed out at the same access control point they entered. When this is not practical, they may sign the person(s) out at a different, designated point.

d. Failure to adhere to the sign-in policy and procedures outlined in AE Regulation 190-16, § 41 and this policy may result in the withdrawal of sign-in privileges and possible administrative actions deemed appropriate by the respective Tailored Garrison/USAG Heidelberg Commander.

e. Personnel will not be signed in as guests for more than the established time limits as directed by the Tailored Garrison Commander. If the visit is of longer duration then both the sponsor and guest(s) will report back to the access control point where the guest was signed in and the sponsor will re-sign in the guest(s).

f. DOD ID card holders must be at least 18 years old to be authorized sign-in privileges.

g. At FPCON Delta, only DOD ID cardholders are authorized sign-in privileges. AE Reg. 190-16, § 12-29, outlines which person categories are authorized sign-in privileges at each FPCON level.

h. Contractors who are granted sign-in privileges are limited to FPCONs Alpha and Bravo only. They must comply with all force protection measures implemented at all times.

i. If the access control point is equipped with IACS the guard will follow the procedures outlined in AE Regulation 190-16. Section VI

j. If the access control point is not equipped with IACS the guard will:

(1) Ensure through visual comparison that the individual being signed in is the person in the photo on their passport or ID card.

(2) Log the individuals being signed in and the sponsor into the visitor log.

(3) Check the bar roster to ensure these individuals are not barred.

12. Access Roster Procedures:

a. Access rosters will be processed IAW procedures outlined in AE Regulation 190-16, § 42. Rosters will include the full name, country of citizenship, passport number or person ID number, and vehicle license plate number, if applicable. Access roster requests can only be signed and submitted by DOD ID cardholders (example: Soldier holding party inviting Local guests submits roster).

b. All access rosters will be completed at the IACO and routed through the Pond SCOR to each Access Control Point. The Pond SCOR will ensure they are complete and contain all required documentation. The SCOR will approve them by annotating “approval” and signature.

c. Special one-time event access rosters will be submitted as outlined above. However, if all information required is not included the requestor will be responsible for vouching for the visitor(s) at the ACP upon their entry.

d. All access control points will maintain paper copies of approved access rosters in the event of power failure or loss of connectivity. Access rosters will be kept on file at the Tailored Garrison IACO for a minimum of 90 days past their expiration date.

13. Procedures for Visiting Family Members or friends in accordance with AE Reg 190-16 § 24:

a. Visitors who will be in USAREUR may be issued an installation pass for the duration of their visit IAW AE Regulation 190-16, § 24.

b. These passes will provide the visitor with unaccompanied access to the Tailored Garrison where it was issued and USAREUR-wide access when accompanied by the sponsoring DOD ID card holder.

c. The DOD ID cardholder who is being visited may prepare AE Form 190-16A, Application for USAREUR/USAFE Installation Pass, by going either to the IACO or Central Processing Facility (CPF).

d. The forms will be forwarded to the Tailored Garrison designated sponsoring authority for approval and returned to the IACO.

e. Upon arrival, the guest(s) will proceed to the IACO or CPF. They must be signed in and escorted to the IACO or CPF by the DOD ID cardholder where they will receive their installation pass.

f. To alleviate the sign-in process, the DOD ID card holder may place the visitor on an access roster for a period covering the day of arrival, or, if necessary any additional days that fall between the arrival date and the time the pass office or CPF opens for business. Pass issued will not exceed the time of the visit or up to 90 days, whichever is less.

14. Procedures for integrating IACS into the AT/FP plan:

a. Commanders can have a more effective installation access control program by utilizing the various aspects of IACS.

b. USAG Heidelberg ATO officer will recommend to the USAG Heidelberg Commander which aspects of IACS to implement at the various FPCON levels.

5 Encls

1. Example 1: Report of Lost/Stolen USAREUR Installation Pass or DOD ID Card
2. Examples 2 and 2a: Request and Response for Military Police Records Check
3. Example 3: Approval or Disapproval Request for Installation Access
4. Attachment 4: Derogatory Information Approval Process
5. Reference List

**Example 1: Report of Lost/Stolen
USAREUR Installation Pass or DOD ID Card**

MEMORANDUM FOR PROVOST MARSHAL, USAG Heidelberg, ATTN: IMEU-HEI-ESP,
APO AE 09102.

SUBJECT: Report of Lost/Stolen USAREUR Installation Pass or DOD ID Card

1. IAW § 7 (Procedures for Lost ID cards and passes), USAG Heidelberg Command Policy Memorandum XX, Access Control, (date), the below named individual is reporting his USAREUR Installation Pass/DOD ID Card has been Lost/Stolen.

a. _____,
LAST NAME / Familienname FIRST NAME / Vorname

b. Passport Number _____
Personalausweis Nummer

c. Date of Birth / Geburtstag _____

d. Place of Birth / Geburtsort _____

e. Nationality _____
Staatsangehoerigkeit

f. Address / Anschrift _____

g. Occupation / Beruf _____

h. Place of Employment _____
Beschaeftigungsort

i. Duty Telephone Number _____
Diensttelefon

Narrative description of loss or theft of card: _____

4. This loss / theft report submitted by: _____

Example 2: Request for Military Police Background Check
Appropriate Letterhead (Entsprechender Briefkopf)

Office Symbol
Büro Kennzeichen

Date
Datum

MEMORANDUM FOR xxx USAG Heidelberg, Provost Marshal Office, ATTN: Admin Section,
APO AE xxxxx

MEMORANDUM FÜR xxx Base Support Battalion, Provost Marshal Office, z. Hd.
Verwaltungsabteilung, APO AE xxxxx

SUBJECT: Request for Military Police Background Check
BETREFF: Antrag auf ein Militäerpolizeiliches Führungszeugnis.

1. The individual named below is employed with (name of sponsoring organization) and is requesting a Military Police background check, as required by AE Regulation 190-16, to meet the requirements to obtain installation pass. (Die unten genannte Person, die bei (Name der bürgernden Organisation) be-schäftigt ist, beantragt ein Militärpolizeiliches Führungszeugnis, wie von Vorschrift AE Reg 190-16 verlangt, um einen Zutrittsausweis zu erhalten).

2. I _____ understand by signing this document, I will have a Military Police background check done on myself. All information found on me, whether negative or positive and reasons thereof, will be released to authorized _____ personnel for consideration of installation pass privileges. (Ich _____ verstehe, dass mit meiner Unterschrift auf diesem Dokument, ein Militärpolizeiliches Führungszeugnis über mich erstellt wird. Alle negativen als auch positiven Vermerke werden an autorisiertes Personal weitergeleitet, die diese Information berücksichtigen werden).

a. Signature / Unterschrift : _____ Date / Datum: _____

b. Date of Birth / Geburtsdatum: _____

c. Place of Birth / Geburtsort: _____

2. POC for this memorandum is (name, grade/rank, phone # and email Address).
Ansprechpartner fuer dieses Memorandum ist (Name, Position/Rang, Telefon Nr. und e-mail adresse.

SIGNATURE BLOCK/UNTERSCHRIFTSBLOCK

**Example 2a: Response to Request for
Military Police Records Check**

MEMORANDUM FOR

Our files reveal that the records on the above named applicant are:

Unsere Ermittlungen ergeben für den oben genannten Antragsteller folgende Aktenvermerke:

___ No derogatory Information

___ Keine negativen Informationen

___ Derogatory Information

___ Negative Informationen

Signature
Unterschrift

Date
Datum

Example 3: Approval or Disapproval Request for Installation Access

APPROPRIATE ORGANIZATION / UNIT LETTERHEAD

AETV SYMBOL

DATE

MEMORANDUM THRU Appropriate Approval Authority

FOR (Local) Tailored Garrison IACO, APO AE 09102

SUBJECT: Approval or Non-Approval of Request for Access Installation

1. The following individual's background check was returned to this office with derogatory information:

a. Name: _____

b. DOB: _____

c. Passport/Ausweis#: _____

2. Derogatory information is listed on attachment.

3. I have reviewed the derogatory information and recommend approval/disapproval for name of applicant to obtain an installation pass.

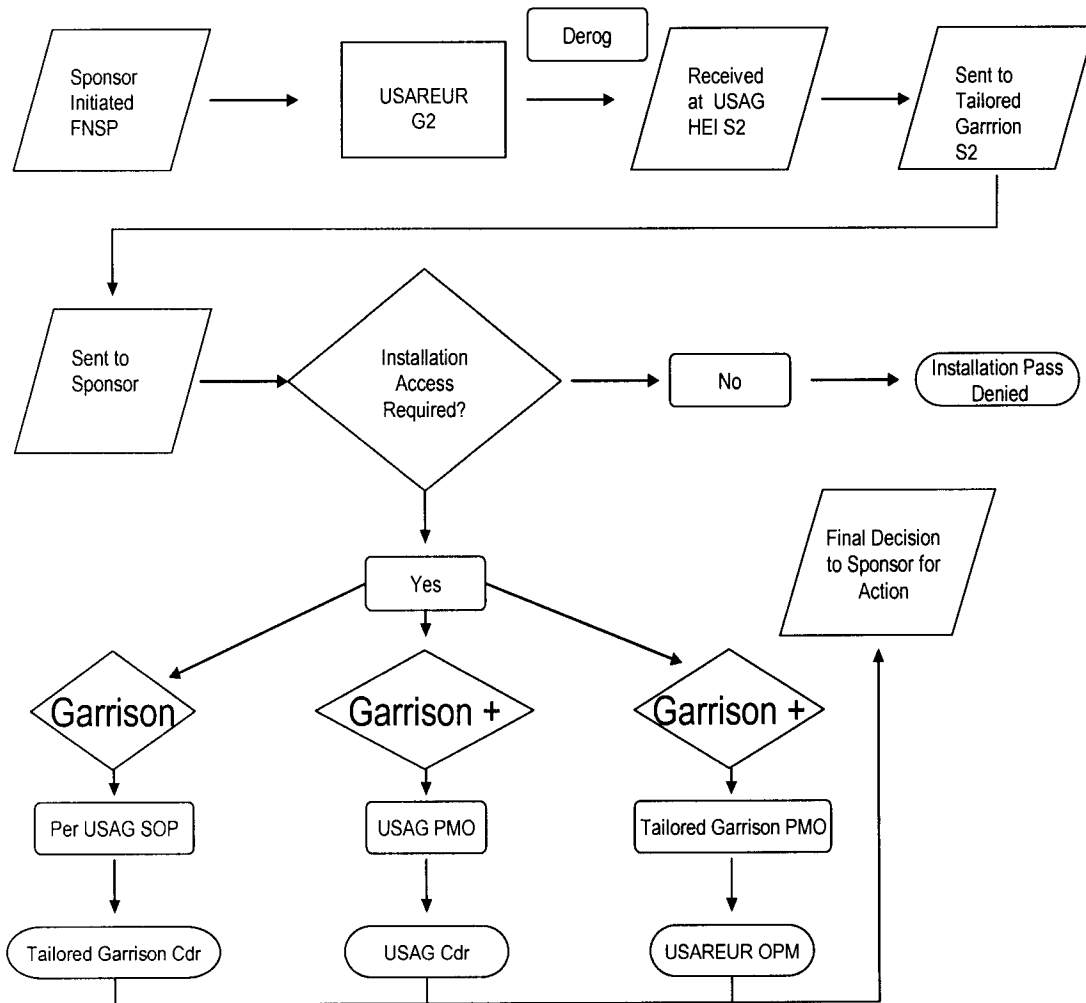
4. POC for this memorandum is _____
(name, rank, phone # and email).

Sponsoring Official's Signature Block

Recommendation is approved/disapproved.

Approval Authority
Signature Block
(leave blank for USAREUR)

Attachment 4: Derogatory Information Approval Process



Reference List:

1. Army Regulation 190-56, the Army Civilian Police and Security Guard Program, 21 Jun 95.
2. Army Regulation 380-67, Personnel Security Program, 9 Sep 98.
3. Army Regulation 190-22, Search and Seizure, 1 Jan 83.
4. Army in Europe Regulation 190-13, The USAREUR Physical Security Program, 23 Oct 03.
5. USAREUR Regulation 525-13, Antiterrorism and Force Protection, 17 Aug 04.
6. USAREUR Regulation 600-700, Identification Cards and Individual Logistical Support, 17 Jul 02.
7. USAREUR Regulation 604-1, Local National Screening Program (Laredo Leader), 27 Jan 94.
8. USAREUR Supplement 1 to AR 190-22, Search and Seizure, 10 Aug 99.
9. USAREUR Supplement 1 to AR 380-67, Personnel Security Program, 20 Jan 94.